CYBER SECURITY

MCQ Questions

1) In which of the following, a person is constantly followed/chased by another person or group of several peoples?

a. Phishing
b. Bulling
c. Stalking
d. Identity theft

Answer: c

Explanation: In general, Stalking refers to continuous surveillance on the target (or person) done by a group of people or by the individual person.

Cyber Stalking is a type of cybercrime in which a person (or victim) is being followed continuously by another person or group of several people through electronic means to harass the victim. We can also say that the primary goal of **Stalking** is to observe or monitor each victim's actions to get the essential information that can be further used for threatening, harassing, etc.

---

2) Which one of the following can be considered as the class of computer threats?

a. Dos Attack
b. Phishing
c. Soliciting
d. Both A and C

Answer: a

Explanation: A dos attack refers to the denial of service attack. It is a kind of cyber attack in which one tries to make a machine (or targeted application, website etc.) unavailable for its intended users. It is usually accomplished by disturbing the service temporarily or indefinitely of the target connected to the internet.

---

3) Which of the following is considered as the unsolicited commercial email?

a. Virus
b. Malware
c. Spam
d. All of the above

Answer: c

Explanation: It is a type of unsolicited email which is generally sent in bulk to an indiscriminate recipient list for commercial purpose. Generally, these types of mail are considered unwanted because most users don't want these emails at all.

---

4) Which of the following usually observe each activity on the internet of the victim, gather all information in the background, and send it to someone else?

a. Malware
b. Spyware
c. Adware
d. All of the above

Answer: b

Explanation: It is generally defined as the software designed to enter the target's device or computer system, gather all information, observe all user activities, and send this information to a third party. Another important thing about the spyware is that it works in the background sends all information without your permission.

---

5) _______ is a type of software designed to help the user's computer detect viruses and avoid them.

a. Malware
b. Adware
c. Antivirus
d. Both B and C

Answer: c

Explanation: An antivirus is a kind of software that is specially designed to help the user's computer to detect the virus as well as to avoid the harmful effect of them. In some cases where the virus already resides in the user's computer, it can be easily removed by scanning the entire system with antivirus help.

---

6) Which one of the following is a type of antivirus program?

a. Quick heal

b. Mcafee

c. Kaspersky

d. All of the above

Answer: d

Explanation: Antivirus is a kind of software program that helps to detect and remove viruses form the user's computer and provides a safe environment for users to work on. There are several kinds of antivirus software are available in the market, such as Kaspersky, Mcafee, Quick Heal, Norton etc., so the correct answer is D.

---

7) It can be a software program or a hardware device that filters all data packets coming through the internet, a network, etc. it is known as the_______:

a. Antivirus

b. Firewall

c. Cookies

d. Malware

Answer: b

Explanation: There are two types of firewalls - software programs and hardware-based firewalls. These types of firewalls filter each and every data packet coming from the outside environment such as network; internet so that any kind of virus would not be able to enter in the user's system. In some cases where the firewall detects any suspicious data packet, it immediately burns or terminates that data packet. In short, we can also say that it is the first line of defense of the system to avoid several kinds of viruses.

---

8) Which of the following refers to stealing one's idea or invention of others and use it for their own benefits?

a. Piracy
b. Plagiarism
c. Intellectual property rights
d. All of the above

Answer: d

Explanation: The stealing ideas or the invention of others and using them for their own profits can also be defined in several different ways, such as piracy, intellectual property rights, and plagiarism.

---

9) Read the following statement carefully and find out whether it is correct about the hacking or not?

It can be possible that in some cases, hacking a computer or network can be legal.

a. No, in any situation, hacking cannot be legal
b. It may be possible that in some cases, it can be referred to as a legal task

Answer: b

Explanation: Nowadays, hacking is not just referred to as an illegal task because there are some good types of hackers are also available, known as an ethical hacker. These types of hackers do not hack the system for their own purposes, but the organization hires them to hack their system to find security falls, loop wholes. Once they find the loop whole or venerability in the system, they get paid, and the organization removes that weak points.

---

10) Which of the following refers to exploring the appropriate, ethical behaviors related to the online environment and digital media platform?

a. Cyber low
b. Cyberethics
c. Cybersecurity
d. Cybersafety

Answer: b

Explanation: Cyber Ethics refers to exploring the appropriate, ethical behaviors related to online environments and digital media.

---

11) Which of the following refers to the violation of the principle if a computer is no more accessible?

a. Access control

b. Confidentiality

c. Availability

d. All of the above

Answer: c

Explanation: Availability refers to the violation of principle, if the system is no more accessible.

---

12) Which one of the following refers to the technique used for verifying the integrity of the message?

a. Digital signature

b. Decryption algorithm

c. Protocol

d. Message Digest

Answer: d

Explanation: Message Digest is a type of cryptographic hash function that contains a string of digits that are created by the one-way hashing formula. It is also known as a type of technique used for verifying the integrity of the message, data or media, and to detect if any manipulations are made. Therefore the correct answer is D.

---

13) Which one of the following usually used in the process of Wi-Fi-hacking?

a. Aircrack-ng

b. Wireshark

c. Norton

d. All of the above

Answer: a

Explanation: The Aircrack-ng is a kind of software program available in the Linux-based operating systems such as Parrot, kali etc. it is usually used by users while hacking the Wi-Fi-networks or finding vulnerabilities in the network to capture or monitor the data packets traveling in the network.

---

14) Which of the following port and IP address scanner famous among the users?

a. Cain and Abel

b. Angry IP Scanner

c. Snort

d. Ettercap

Answer: b

Explanation: Angry IP Scanner is a type of hacking tool that is usually used by both white hat and black hat types of hackers. It is very famous among the users because it helps to find the weaknesses in the network devices.

---

15) In ethical hacking and cyber security, there are _______ types of scanning:

a. 1

b. 2

c. 3

d. 4

Answer: c

Explanation: There are usually three types of scanning in ethical hacking and cyber security. Therefore the correct answer is C.

---

16) Which of the following is not a type of scanning?

a. Xmas Tree Scan
b. Cloud scan
c. Null Scan
d. SYN Stealth

Answer: b

Explanation: Among the following-given options, the Cloud Scan is one, and only that is not a type of scanning.

---

17) In system hacking, which of the following is the most crucial activity?

a. Information gathering
b. Covering tracks
c. Cracking passwords
d. None of the above

Answer: c

Explanation: While trying to hack a system, the most important thing is cracking the passwords.

---

18) Which of the following are the types of scanning?

a. Network, vulnerability, and port scanning
b. Port, network, and services
c. Client, Server, and network
d. None of the above

Answer: a

Explanation: The vulnerability, port, and network scanning are three types of scanning.

---

19) Which one of the following is actually considered as the first computer virus?

a. Sasser
b. Blaster
c. Creeper
d. Both A and C

Answer: c

Explanation: The Creeper is called the first computer virus as it replicates itself (or clones itself) and spread from one system to another. It is created by Bob Thomas at BBN in early 1971 as an experimental computer program.

---

20) To protect the computer system against the hacker and different kind of viruses, one must always keep _________ on in the computer system.

a. Antivirus
b. Firewall
c. Vlc player
d. Script

Answer: b

Explanation: It is essential to always keep the firewall on in our computer system. It saves the computer system against hackers, viruses, and installing software form unknown sources. We can also consider it the first line of defense of the computer system.

---

21) Code Red is a type of ________

a. An Antivirus Program
b. A photo editing software
c. A computer virus
d. A video editing software

Answer: c

Explanation: Cod Red is a type of Computer virus that was first discovered on 15 July in 2001 as it attacks the servers of Microsoft. In a couple of next days, it infects almost 300,000 servers.

---

22) Which of the following can be considered as the elements of cyber security?

a. Application Security

b. Operational Security

c. Network Security

d. All of the above

Answer: d

Explanation: Application security, operational security, network security all are the main and unforgettable elements of Cyber Security. Therefore the correct answer is D.

---

23) Which of the following are famous and common cyber-attacks used by hackers to infiltrate the user's system?

a. DDos and Derive-by Downloads

b. Malware & Malvertising

c. Phishing and Password attacks

d. All of the above

Answer: d

Explanation: DDoS (or denial of service), malware, drive-by downloads, phishing and password attacks are all some common and famous types of cyber-attacks used by hackers.

---

24) Which one of the following is also referred to as malicious software?

a. Maliciousware

b. Badware

c. Ilegalware

d. Malware

Answer: d

Explanation: Malware is a kind of short program used by the hacker to gain access to sensitive data/ information. It is used to denote many kinds of viruses, worms, Trojans, and several other harmful programs. Sometimes malware is also known as malicious software.

---

25) Hackers usually used the computer virus for ______ purpose.

a. To log, monitor each and every user's stroke

b. To gain access the sensitive information like user's Id and Passwords

c. To corrupt the user's data stored in the computer system

d. All of the above

Answer: d

Explanation: In general, hackers use computer viruses to perform several different tasks such as to corrupt the user's data stored in his system, to gain access the important information, to monitor or log each user's strokes. Therefore the correct answer is D.

---

26) In Wi-Fi Security, which of the following protocol is more used?

a. WPA

b. WPA2

c. WPS

d. Both A and C

Answer: b

Explanation: Nowadays, in Wi-Fi Security, the WPA2 is one of the most widely used protocols because it offers a more secure connection rather than the WPA. It is also known as the upgraded version of the WPA protocol.

---

27) The term "TCP/IP" stands for_____

a. Transmission Contribution protocol/ internet protocol

b. Transmission Control Protocol/ internet protocol

c. Transaction Control protocol/ internet protocol

d. Transmission Control Protocol/ internet protocol

Answer: b

Explanation: The term "TCP/IP" stood for Transmission Control Protocol/ internet protocol and was developed by the US government in the early days of the internet.

---

28) The response time and transit time is used to measure the ____________ of a network.

a. Security

b. Longevity

c. Reliability

d. Performance

Answer: d

Explanation: On the basis of response time and transit time, the performance of a network is measured.

---

29) Which of the following factor of the network gets hugely impacted when the number of users exceeds the network's limit?

a. Reliability

b. Performance

c. Security

d. Longevity

Answer: d

Explanation: When the numbers of users on a network get increased and exceed the network's limit, therefore the performance is one of the factors of the network that is hugely impacted by it.

---

30) In the computer networks, the encryption techniques are primarily used for improving the ________

a. Security

b. Performance

c. Reliability

d. Longevity

Answer: a

Explanation: Encryption techniques are usually used to improve the security of the network. So the correct answer will be A.

---

31) Which of the following statements is correct about the firewall?

a. It is a device installed at the boundary of a company to prevent unauthorized physical access.

b. It is a device installed at the boundary of an incorporate to protect it against the unauthorized access.

c. It is a kind of wall built to prevent files form damaging the corporate.

d. None of the above.

Answer: b

Explanation: A firewall can be the type of either a software or the hardware device that filters each and every data packet coming from the network, internet. It can also be considered as a device installed at the boundary of an incorporate to protect form unauthorized access. Sometimes firewall also refers to the first line of defense against viruses, unauthorized access, malicious software etc.

---

32) When was the first computer virus created?

a. 1970

b. 1971

c. 1972

d. 1969

Answer: b

Explanation: In 1970, the world's first computer virus was created by Robert (Bob) Thomas. This virus was designed as it creates copies of itself or clones itself and spreads one computer to another. So the correct answer will be 1970.

---

33) Which of the following is considered as the world's first antivirus program?

a. Creeper
b. Reaper
c. Tinkered
d. Ray Tomlinson

Answer: b

Explanation: Reaper is considered as the world's first antivirus program or software as it can detect the copies of a Creeper (the world's first man-made computer virus) and could delete it as well.

---

34) Which one of the following principles of cyber security refers that the security mechanism must be as small and simple as possible?

a. Open-Design
b. Economy of the Mechanism
c. Least privilege
d. Fail-safe Defaults

Answer: b

Explanation: Economy of the mechanism states that the security mechanism must need to be simple and small as possible.

---

35) Which of the following principle of cyber security restricts how privileges are initiated whenever any object or subject is created?

a. Least privilege

b. Open-Design

c. Fail-safe Defaults

d. None of the above

Answer: c

Explanation: The fail-safe Defaults principle of cyber security restricts how privileges are initiated whenever a subject or object is created. In cases where the privileges, rights, access or some other security-related attribute is not granted explicitly, it should also not granted access to the object.

---

36) Suppose an employee demands the root access to a UNIX system, where you are the administrator; that right or access should not be given to the employee unless that employee has work that requires certain rights, privileges. It can be considered as a perfect example of which principle of cyber security?

a. Least privileges

b. Open Design

c. Separation of Privileges

d. Both A & C

Answer: a

Explanation: The example given in the above question refers to the least privileges principle of cyber security. The least privileges principle of cyber security states that no rights, access to the system should be given to any of the employees of the organization unless he/she needs those particular rights, access in order to complete the given task. In short, we can say that its primary work is to restrict or control the assignment of rights to the employees.

---

37) Which of the following can also consider as the instances of Open Design?

a. CSS

b. DVD Player

c. Only A

d. Both A and B

Answer: d

Explanation: The Open Design is a kind of open design artifact whose documentation is publically available, which means anyone can use it, study, modify, distribute, and make the prototypes. However, the CSS (or Content Scrambling System) and DVD Player are both examples of open design.

---

38) Which one of the following principles states that sometimes it is become more desirable to rescored the details of intrusion that to adopt more efficient measure to avoid it?

a. Least common mechanism

b. Compromise recording

c. Psychological acceptability

d. Work factor

Answer: b

Explanation: The principle called compromise factor states that in some cases, it is more beneficial to records or document the details of the intrusion that to adopt more efficient measures to avoid it.

---

39) The web application like banking websites should ask its users to log-in again after some specific period of time, let say 30 min. It can be considered as an example of which cybersecurity principle?

a. Compromise recording

b. Psychological acceptability

c. Complete mediation

d. None of the above

Answer: c

Explanation: The complete mediation principle of cybersecurity requires that all the access must be checked to ensure that they are genuinely allowed. However, the example given in the above question can be considered as an example of Complete Mediation.

---

40) Which one of the following statements is correct about Email security in the network security methods?

a. One has to deploy hardware, software, and security procedures to lock those apps down.

b. One should know about what the normal behavior of a network look likes so that he/she can spot any changes, breaches in the behavior of the network.

c. Phishing is one of the most commonly used methods that are used by hackers to gain access to the network

d. All of the above

Answer: c

Explanation: In terms of Email Security, phishing is one of the standard methods that are used by Hackers to gain access to a network. The Email Security Tools can handle several types of attacks, such as the incoming attacks, and protect the outbound messages containing sensitive data/information as well.

---

41) Which of the following statements is true about the VPN in Network security?

a. It is a type of device that helps to ensure that communication between a device and a network is secure.

b. It is usually based on the IPsec(IP Security) or SSL (Secure Sockets Layer)

c. It typically creates a secure, encrypted virtual "tunnel" over the open internet

d. All of the above

Answer: d

Explanation: The term VPN stands for Virtual Private Network. It is a type of network security-enhancing tool that can be either a software program or a hardware device. It usually authenticates the communication between a device and a network by creating a secure encrypted virtual "tunnel". In general, the software VPNs are considered as the most cost-effective, user friendly over the hardware VPNs.

---

42) Which of the following type of text is transformed with the help of a cipher algorithm?

a. Transformed text

b. Complex text

c. Scalar text

d. Plain text

Answer: d

Explanation: The cipher algorithm is used to create an encrypted message by taking the input as understandable text or "plain text" and obtains unreadable or "cipher text" as output. It is usually used to protect the information while transferring one place to another place.

---

43) The term "CHAP" stands for __________

a. Circuit Hardware Authentication Protocols

b. Challenge Hardware Authentication Protocols

c. Challenge Handshake Authentication Protocols

d. Circuit Handshake Authentication Protocols

Answer: c

Explanation: The term "CHAP" stands for the Challenge Handshake Authentication Protocols. In computer networks, it can be defined as an authentication scheme that avoids the transfer of unencrypted passwords over the network. The "CHAP" is one of the many authentication schemes used by the Point To Point Protocol (PPP), which is a serial transmission protocol for wide networks Connections (WAN).

---

44) Which type of the following malware does not replicate or clone them self's through infection?

a. Rootkits

b. Trojans

c. Worms

d. Viruses

Answer: b

Explanation: The Trojans type of malware does not generate copies of them self's or clone them. The main reason why these types of viruses are referred to as the Trojans is the mythological story of the Greeks. In which some top-level accessions were hidden in the big wooden horse-like structure and given to the enemy as a gift. So that they can enter to the enemy's palace without come in any sight.

---

45) Which of the following malware's type allows the attacker to access the administrative controls and enables his/or her to do almost anything he wants to do with the infected computers.

a. RATs
b. Worms
c. Rootkits
d. Botnets

Answer: a

Explanation: The RAT is an abbreviation of Remote Access Trojans or Remote Administration Tools, which gives the total control of a Device, which means it, can control anything or do anything in the target device remotely. It allows the attacker administrative control just as if they have physical access to your device.

---

46) Which of the following statements is true about the Trojans?

a. Trojans perform tasks for which they are designed or programmed
b. Trojans replicates them self's or clone them self's through an infections
c. Trojans do nothing harmful to the user's computer systems
d. None of the above

Answer: a

Explanation: Trojans are a type of malware that will perform any types of actions for those they are design or programmed. Another important thing about Trojans is that the user may not know that the malware enters their system until the Trojan starts doing its job for which they are programmed.

---

47) Which of the following is just opposite to the Open Design principle?

a. Security through obscurity

b. Least common mechanism

c. Least privileges

d. Work factor

Answer: a

Explanation: The "Security through obscurity" is an approach which just opposite to the Open Design principle. So the correct option is A.

---

48) Which of the following is a type of independent malicious program that never required any host program?

a. Trojan Horse

b. Worm

c. Trap Door

d. Virus

Answer: b

Explanation: Warm is a type of independent malicious program that does not require any host programs(or attached with some programs). They typically cause damages to the systems by consuming the bandwidths and overloading the servers. Warms are quite different from the virus as they are stand-alone programs, whereas viruses need some type of triggers to activate by their host or required human interaction.

---

49) Which of the following usually considered as the default port number of apache and several other web servers?

a. 20

b. 40

c. 80

d. 87

Answer: c

Explanation: The default port number used by the apache and several other web servers is 80. So the correct answer will be C.

50) DNS translates a Domain name into _________

a. Hex

b. Binary

c. IP

d. URL

Answer: d

Explanation: DNS stands for the Domain name system; the main work of a DNS is to translate the Domain name into an IP address that is understandable to the computers.

51) Which one of the following systems cannot be considered as an example of the operating systems?

a. Windows 8

b. Red Hat Linux

c. BSD Linux

d. Microsoft Office

Answer: d

Explanation: Microsoft office is a type of software used for creating and managing documents, which is one of the most famous products of the Microsoft organization. So the correct answer will be the D.

52) In the CIA Triad, which one of the following is not involved?

a. Availability

b. Confidentiality

c. Authenticity

d. Integrity

Answer: c

Explanation: CIA refers to Confidentiality, Integrity, and Availability that are also considered as the CIA triad. However, the CIA triad does not involve Authenticity.

---

53) In an any organization, company or firm the policies of information security come under__________

a. CIA Triad
b. Confidentiality
c. Authenticity
d. None of the above

Answer: a

Explanation: Confidentiality, Integrity, Availability are the three main principles. In Short, these three principles are also known as the CIA triad and plays a vital role as the cornerstone of the security structure of any organization.

---

54) Why are the factors like Confidentiality, Integrity, Availability, and Authenticity considered as the fundamentals?

a. They help in understanding the hacking process
b. These are the main elements for any security breach
c. They help to understand the security and its components in a better manner
d. All of the above

Answer: c

Explanation: Confidentiality, Integrity, Availability and Authenticity all these four elements helps in understanding security and its components.

---

55) In order to ensure the security of the data/ information, we need to ____________ the data:

a. Encrypt
b. Decrypt
c. Delete

d. None of the above

Answer: a

Explanation: Data encryption is a type of method in which the plain text is converted into ciphertext, and only the authorized users can decrypt it back to plain text by using the right key. This preserves the Confidentiality of the Data.

---

56) Which one of the following is considered as the most secure Linux operating system that also provides anonymity and the incognito option for securing the user's information?

a. Ubuntu

b. Tails

c. Fedora

d. All of the above

Answer: b

Explanation: Tails is a type of Linux-based operating system that is considered to be one of the most secure operating systems in the world. It also provides many features such as anonymity and incognito options to insure that user information is always protected. The main reason why the tails operating system is famous among the user is that it is almost untraceable, which keep your privacy secure.

---

57) Which type following UNIX account provides all types of privileges and rights which one can perform administrative functions?

a. Client

b. Guest

c. Root

d. Administrative

Answer: d

Explanation: If a user uses the Root account of the UNIX operating system, he can carry out all types of administrative functions because it provides all necessary privileges and rights to a user.

---

58) Which of the following is considered as the first hacker's conference?

a. OSCON
b. DEVON
c. DEFCON
d. SECTION

Answer: c

Explanation: DEFCON is one of the most popular and largest Hacker's as well as the security consultant's conference. It is always held once a year in Las Vegas, Nevada, where hackers of all types (such as black hats, gray hats, and white hat hackers), government agents as well as security professionals from around the world attend the conference attends this meeting.

---

59) Which of the following known as the oldest phone hacking techniques used by hackers to make free calls?

a. Phreaking
b. Phishing
c. Cracking
d. Spraining

Answer: a

Explanation: Phreaking is considered as one of the oldest phone hacking techniques used by hackers to make free calls.

---

60) Name of the Hacker who breaks the SIPRNET system?

a. John Draper
b. Kevin Mitnick
c. John von Neumann
d. Kevin Poulsen

Answer: d

Explanation: The SIPRNET (or Advanced Research Project Agency Network) system was first hacked by Kevin Poulsen as he breaks into the Pentagon network.